LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATES

Abstract of the Disclosure

A public key infrastructure (PKI) includes a subject, a verifier, and certificate authority that issues a first unsigned certificate to the subject that binds a public key of the subject to long-term identification information related to the subject and maintains a certificate database of unsigned certificates in which it stores the first unsigned certificate. The verifier maintains a hash table containing cryptographic hashes of valid unsigned certificates corresponding to the unsigned certificates stored in the certificate database and including a cryptographic hash of the first unsigned certificate. The subject presents the issued first unsigned certificate to the verifier for authentication and demonstrates that the subject has knowledge of a private key corresponding to the public key in the unsigned certificate.